

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED
MAR 30 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)
)
Implementation of the)
Telecommunications Act of 1996:)
)
Telecommunications Carriers' Use of)
Customer Proprietary Network Information)
And Other Customer Information)

CC Docket No. 96-115

**COMMENTS OF
THE ALARM INDUSTRY COMMUNICATIONS COMMITTEE**

The Alarm Industry Communications Committee ("AICC"), by its attorneys, respectfully submits the following comments in response to the Commission's *Further Notice of Proposed Rulemaking* in the above captioned docket.¹ For the reasons explained below, AICC urges the Commission to adopt rules to protect against unlawful use of customer proprietary network information ("CPNI") in violation of Section 275(d) of the Act.

I. SUMMARY

The *Further Notice* seeks additional comments on enforcement mechanisms to ensure the confidentiality of CPNI and on additional safeguards to protect the confidentiality of a competing carriers' information, including information services providers (such as alarm monitoring providers). The AICC, a trade group dedicated to the communications needs of alarm monitoring providers, recommends that the FCC adopt a rule to safeguard against

¹ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, FCC 98-27 (rel. Feb. 26, 1998) (*Further Notice*).

improper access to alarm monitoring data by local exchange carrier ("LEC") personnel marketing alarm monitoring services. Specifically, to protect against improper disclosure of Section 275(d) alarm monitoring data through LEC access to CPNI call detail, the Commission should require LECs to restrict its alarm monitoring personnel from accessing CPNI call detail records of local exchange subscribers. This proposal is similar to AICC's earlier proposal in this docket but with one significant change: LEC personnel would be denied access to call detail records, but not other CPNI not containing information on the occurrence or contents of calls.

Such a rule is appropriate because (1) LECs are prohibited from accessing alarm monitoring data to market alarm monitoring services, even with customer consent, (2) information concerning the occurrence or contents of calls to alarm providers (Section 275 alarm data) will be contained in CPNI call detail records, and (3) there is no feasible way to screen this information without collecting the very data LECs are prohibited from using. The Commission acknowledged that AICC's previous proposal was one way to ensure compliance with Section 275(d) and the CPNI rules, although it declined to adopt the rule on the belief that other alternatives might also protect such information. No LECs have offered any such alternatives, and, moreover, AICC has reduced the scope of its proposal to include only call detail records, where alarm monitoring data is most likely to reside. Accordingly, AICC urges the FCC to adopt its proposal at this time.

II. BACKGROUND

The AICC is a subcommittee of the Central Station Alarm Association ("CSAA"), a national industry group promoting the general, commercial and regulatory interests of the nation's central station alarm monitoring service providers. The AICC represents alarm monitoring providers in proceedings before various federal government agencies and courts,

including the FCC. AICC frequently has participated in this Commission's CPNI proceedings, including proceedings in the above-captioned docket.

In June of 1996, AICC submitted comments in response to the Commission's *Notice of Proposed Rulemaking* in this docket. In those comments, AICC pointed out that Congress prohibited in all instances the use of alarm monitoring data by a LEC for purposes of marketing alarm monitoring services.² Alarm monitoring data can be stored in any number of locations in a LEC's records, including in individually-identifiable subscriber records constituting CPNI. Therefore, AICC urged the Commission to rule that where information constituted both CPNI and alarm monitoring data, both statutory restrictions applied cumulatively.³ For example, if a LEC obtained customer approval to use CPNI for marketing purposes, that approval would *not* authorize the LEC to use information in that CPNI identifying "the occurrence or contents of calls" to alarm monitoring providers for purposes of marketing an alarm monitoring service to the customer. AICC further recommended that, to ensure compliance with Section 275(d)'s prohibition, the Commission's CPNI rules should require LECs to deny CPNI access to their personnel (or personnel of their affiliates) responsible for marketing alarm monitoring services.⁴

On August 7, 1996, the Commission released a *Report and Order* in this proceeding agreeing with AICC's interpretation of the alarm data provisions of the Act.⁵ The

² AICC Comments at 5 (June 11, 1996); *see* 47 U.S.C. § 275(d). Alarm monitoring data is defined as information concerning "the occurrence or contents of calls received by providers of alarm monitoring services." *Id.*

³ AICC Comments at 6.

⁴ *Id.* at 6-7.

⁵ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information; Use of Data Regarding Alarm*
(continued...)

Commission concluded “that Section 275(d) restricts LEC personnel from using information regarding ‘the occurrence or content of calls received by providers of alarm monitoring services’ for the purpose of marketing their own alarm monitoring service, or an alarm monitoring service offered by another affiliated or unaffiliated entity.”⁶ The Commission noted that alarm monitoring data may also constitute CPNI, and affirmed that “even if a carrier has received customer authorization to obtain access to CPNI pursuant to Section 222(c)(1), such authorization does not extend to any CPNI subject to the Section 275(d) ban”⁷ Although the Commission decided not to adopt regulations to enforce Section 275(d) in the Order, it noted that AICC’s proposal “sets forth one method by which LECs may ensure that they are in compliance with Section 275(d).”⁸ The Commission stated that it would examine “whether any restrictions on access to CPNI are necessary to effectuate the Section 275(d) prohibition at the same time [it] examine[s] whether to impose specific safeguards to protect against unauthorized disclosure of restricted CPNI.”⁹

In the *Further Notice*, the Commission resolved a number of pending CPNI issues, including the instances in which customer authorization is necessary to use CPNI and the form and content of such authorization.¹⁰ The Commission asked for further comment, however, regarding safeguards that should be adopted to protect the confidentiality of CPNI. Specifically,

(...continued)

Monitoring Service Providers, Report and Order, 11 FCC Rcd 9553 (1996) (*Alarm Order*).

⁶ *Id.* at 9557.

⁷ *Id.*

⁸ *Id.* at 9558.

⁹ *Id.*

¹⁰ *Further Notice*, at ¶¶ 21-26, 86-87.

the Commission asked whether safeguards were necessary to protect information relating to competing carriers, including information service providers.¹¹ The Commission also asked for comment on additional enforcement mechanisms that could be adopted to ensure carrier compliance with the CPNI rules.¹² AICC submits these comments in response to those requests.

III. SAFEGUARDS ARE NECESSARY TO PROTECT AGAINST UNAUTHORIZED USE OF ALARM MONITORING DATA

In the *Alarm Order*, the Commission affirmed that the CPNI rules do not and cannot override Section 275(d)'s flat prohibition on the use of alarm monitoring data for marketing purposes. In instances where CPNI contains alarm monitoring data, a LEC's use of such information must comply with both Section 275(d) and Section 222.¹³ CPNI access safeguards, therefore, must be consistent with Section 275(d) and must not permit LECs to access alarm monitoring data for purposes of marketing alarm monitoring services.

Moreover, appropriate safeguards for alarm monitoring data must recognize the unique features of the overlap between CPNI and alarm monitoring data:

1. Customers may not waive the restriction on use of alarm monitoring data.

Section 275(d) prohibits the use of "the occurrence or contents of calls" for purposes of marketing alarm monitoring services. Unlike Section 222's CPNI restriction, Section 275(d) does not permit such use even upon customer consent. Thus, there are no circumstances in which a LEC will have a legitimate need to access alarm monitoring data to market alarm monitoring services.

¹¹ *Id.* at ¶ 206.

¹² *Id.* at ¶ 207.

¹³ *Alarm Order*, 11 FCC Rcd at 9557; *Further Notice* at ¶ 8 n.41.

2. Alarm monitoring data will be recorded in call detail records. Clearly, Section 222 and 275(d) overlap. Information concerning the “occurrence or contents of calls” will in most instances also constitute CPNI, if associated with an individual subscriber’s account.¹⁴ Notably, many businesses and alarm customers with specialized security concerns may use routine testing to verify the integrity of the connection to the alarm provider’s central office. This testing most frequently occurs in the form of one or more calls placed at designated intervals (usually at least once per day) from the subscriber location. Under these arrangements, alarm monitoring call records will be created at regular intervals and included in customer CPNI call detail records. Even for other customers, however, outbound call records will be created whenever a customer experiences a fire, burglary or other event (including false alarms) triggering a call to an alarm provider’s central station.

3. Alarm monitoring data may be located in any subscriber’s records, not just in those of an alarm monitoring provider. When a call is placed from a customer premises to an alarm monitoring central station, that fact is associated in at least two CPNI records. Information on the “occurrence or content” of the call not only will be present in the CPNI of the alarm monitoring provider (in the form of incoming call records), but also in the records of each of its customers. Thus, a LEC could obtain prohibited alarm monitoring data not only by reviewing the CPNI of alarm providers, but also by canvassing outbound call records of customers who have given consent to CPNI use. It is not feasible, therefore, to prevent unauthorized use of alarm monitoring data by identifying and segregating alarm provider CPNI records. This problem is exacerbated by the fact that alarm monitoring data will be intermingled with other call records, making it very difficult to excise alarm data from within a customer’s CPNI, either.

¹⁴ Even use of aggregate alarm monitoring data is prohibited by Section 275(d).

AICC submits that the simplest and best method of ensuring protection for alarm monitoring data is to prohibit LEC personnel marketing alarm monitoring services from accessing any call detail information contained in CPNI records. This proposal is similar to that recommended by AICC in 1996, but is narrowed in one significant respect: under AICC's proposal today, LEC alarm marketing personnel may access *other* CPNI, so long as all call detail information is screened from the record.

Implementation of such a system should be relatively straightforward. A LEC would need to develop procedures and/or systems (such as password/ID) to restrict access to call detail records by those persons who are responsible for marketing alarm monitoring services. Other CPNI not containing information on the occurrence or contents of calls may be accessed by LEC personnel in accordance with the CPNI rules, but call records must be blocked for those persons marketing alarm services. For instance, Ameritech (the only BOC permitted to provide alarm monitoring services at this time) currently operates through a subsidiary separate from its local exchange operating companies. Thus, personnel from Ameritech's alarm monitoring subsidiary would be denied access to systems containing local exchange call detail records. On the other hand, Ameritech local exchange personnel, who are not involved in marketing Ameritech's alarm monitoring services, could continue to access CPNI in accordance with the rules and limitations adopted in the *Further Notice*. No customer, therefore, need have his or her ability to control CPNI for non-alarm monitoring purposes hindered by restrictions to implement Section 275(d).

Importantly, AICC's proposal does not prohibit LECs from using CPNI that does not also constitute alarm monitoring data. A LEC may provide its personnel, including personnel marketing alarm monitoring services, with access to non-call detail CPNI, assuming

customer consent is obtained. AICC narrowly limits its proposal to the type of CPNI – call detail records – most likely to contain information concerning the occurrence or contents of calls to alarm monitoring providers. Prohibition on access to these records, rather than screening of the data, is preferable because it does not require a LEC to compile the prohibited information in order to comply with the rule.¹⁵

Finally, AICC reiterates that LECs are free to suggest alternative means of protecting alarm monitoring data from unauthorized use. If a LEC can demonstrate that alarm monitoring data is adequately screened from alarm monitoring personnel and that it sufficiently protects against uses that violate Section 275(d), the Commission may entertain a request for waiver of the access restriction. Unless equivalent protections are put in place, however, the Commission should require LECs to deny their alarm monitoring personnel access to call detail CPNI.

The Commission has acknowledged that AICC's previous proposed access restriction is one way in which LECs may ensure compliance with both Section 275(d) and the CPNI rules.¹⁶ The revised proposal – which prohibits access only to call detail records – also safeguards compliance of Section 275(d) data. By limiting the potential exposure of marketing personnel to call detail records likely to contain prohibited alarm monitoring data, the Commission reduces the risk of violations of Section 275(d). This will provide customers and competing alarm monitoring providers with additional assurance that a LEC is not gaining an

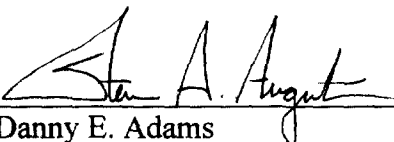
¹⁵ Any system in which alarm monitoring data is screened from CPNI would necessarily require the LEC to compile the phone numbers used by alarm monitoring providers in order to block out call records to or from those numbers. Not only might this be a burdensome undertaking, but it also creates significant risks that the data might be compromised by unauthorized access.

¹⁶ *Alarm Order*, 11 FCC Rcd at 9558.

unfair advantage by virtue of its knowledge of the occurrence or contents of calls to alarm monitoring providers. The Commission declined to mandate a similar proposal by AICC in 1996, based on a belief that alternative, less burdensome methods of ensuring compliance might be available. However, no LEC has come forward with such an alternative, and the Commission does not have any other proposals before it at this time. The Commission should not sacrifice all protection simply because LECs have failed to identify their plans (if any) for protecting alarm monitoring data from unauthorized use. Moreover, AICC has presented a reasonable proposal, employing an approach that avoids harm to legitimate uses of CPNI while protecting against potentially dangerous collections of the very data that may not be used. Accordingly, AICC urges the Commission to adopt its proposed safeguard at this time.

Respectfully submitted,

ALARM INDUSTRY COMMUNICATIONS
COMMITTEE

By: 
Danny E. Adams
Steven A. Augustino
KELLEY DRYE & WARREN LLP
1200 Nineteenth Street, N.W., Suite 500
Washington, D.C. 20036
(202)-955-9600

March 30, 1998

Its Attorneys